PARALLEL KEYSTREAM DECODER

ABSTRACT

Methods and circuitry are disclosed for decoding a keystream. A set of test bits is generated, and a set of attempted keystream bits are generated from differences between the test bits and an input set of cipher bits. A set of current keystream bits are generated from a current seed using a parallel feedback shift register, and the attempted keystream bits are compared to the current keystream bits. In response to attempted keystream bits being equal to the current keystream bits, the current keystream bits are fed back as a new current seed. In response to attempted keystream bits being not equal to the current keystream bits, the attempted keystream bits are fed back as the new current seed.

1